





HOW INTERNATIONAL BUSINESSES COPE WITH TERRORISM

Susanna W. Purnell

December 1986



DISTRIBUTION STATEMENT A

Approved for public releases

Distribution Unlimited

The RAND Corporation

Papers are issued by The RAND Corporation as a service to its professional staff. Their purpose is to facilitate the exchange of ideas among those who share the author's research interests; Papers are not reports prepared in fulfillment of RAND's contracts or grants. Views expressed in a Paper are the author's own and are not necessarily shared by RAND or its research sponsors.

The RAND Corporation, 1700 Main Street, P.O. Box 2138, Santa Monica, CA 90406-2138

HOW INTERNATIONAL BUSINESSES COPE WITH TERRORISM1

Several years ago, Eleanor Wainstein, a RAND colleague, and I did a study for the U.S. Department of Commerce to determine how U.S. businesses cope with the threat of terrorism.² One result of that report is that I am speaking to you tonight. So, I would like to make a few preliminary remarks about that study, since it serves as the basis for much of what I have to say.

We concentrated our study on U.S. business experiences in Latin America, especially two countries which had episodes of severe terrorist threats against business—Argentina and El Salvador. We then gathered data on the experiences of U.S. corporations, including interviews with 40 executives, security officers, and overseas managers of 33 corporations. We also drew on material we had collected for a series of case studies on diplomatic kidnappings in Latin America.

Unfortunately, a planned trip to El Salvador was canceled because of--you guessed it--terrorism. However, we were able to greet many American managers returning from El Salvador virtually as they arrived at the airport and so obtained some pretty vivid reports of the situation. What interested us about El Salvador and Argentina was the fact that while businesses were under heavy terrorist attack, the local government was unable and/or unwilling to help them combat the threat. In other words, businesses were on their own. Thus, the strategies they devised to meet the situation are a kind of acid test of U.S. firms' ability to cope with terrorism, a test, I might add, that they passed with flying colors. But more about that later.

10.

A-1

¹Speech to the Kansas City International Trade Club, November 20, 1986.

²See Susanna W. Purnell and Eleanor Wainstein, *The Problems of U.S. Businesses Operating Abroad in Terrorist Environments*, The RAND Corporation, R-2842-DOC, November 1981.

I am going to deal with four issues tonight. First, why and where terrorists attack businesses. Second, the strategies that American firms have employed to counter those threats. Third, the costs to the firm of both the terrorist attacks and the company's response. And, finally, because I understand there is interest in this topic, I will make some observations on the hostage experience. But, first, let me describe an actual incident which may help to clarify why American businesses can be popular targets.

WHY AND WHERE TERRORISTS ATTACK

On December 6, 1973, the People's Revolutionary Army kidnapped Victor Samuelson, the American manager of the Exxon refinery in Argentina. To gain his release five months later, Exxon paid a record-breaking ransom of \$14.2 million dollars. In addition, the company publishes a communique stating that the ransom was an indemnity "for the super profits that Exxon obtained in the country, thanks to the exploitation of its workers." The terrorists, in turn, announced that nearly half the ransom would go to a Revolutionary Coordination Board, to support terrorist groups in Argentina, Bolivia, Uruguay, and Chile.

Samuelson's kidnapping illustrates many of the reasons terrorists consider businesses such attractive targets. First, it is compatible with the ideological goals of leftist guerrillas to attack the exploiters of the masses. In this instance, raising the specter of "Yankee imperialism" also played on nationalistic feelings.

Second, the publicity attendant on a successful operation often embarrasses the local government and enhances the perceptions of the terrorists. Terrorists can use the public relations aspects of terrorist acts not only to underline the helplessness of the government to prevent terrorism but also to broaden popular support and sympathy. For example, Latin American terrorists in particular have extorted companies into publishing manifestos, distributing food and medical supplies, rehiring laid-off workers, and raising wages.

Third, and most important, terrorists rob, extort, and kidnap for financial gain. Terrorism is an expensive occupation. To support their operations, terrorists must buy arms and equipment, provide safe houses

and transport, and also support group members. Successful terrorist fund-raising activities can mean double trouble for businesses because criminals often imitate their methods, placing the blame on the terrorists while cashing in on their credibility.

In addition, terrorists have, on rare occasions, attached political and economic goals to their attacks on business. For example, the same Revolutionary People's Army made political demands when they kidnapped the general manager of Fiat Concord. Not only did the Argentine government reject the demand for the release of 50 guerrilla prisoners, but the government forbade the company from complying with the kidnappers' demand to rehire fired workers. Ultimately, the captors killed the hostage when police discovered their hideout. Political attacks on businesses to gain political concessions have rarely succeeded.

As final acts of desperation, terrorists have waged economic warfare by attacking the infrastructure, running campaigns to disrupt the labor force, and sabotaging plants. El Salvador's fishing industry had to dump most of its catch after terrorists cut power lines to prevent refrigeration. While disruptive, such attacks have rarely succeeded in the long term.

Finally, businesses often become targets of tactical convenience. As the threat increases, so does the protection surrounding government officials and the diplomatic community. Terrorists then often turn to foreign and local businessmen, a switch in strategy that not only increases the number of targets available but usually means easier, less well-protected targets.

In the way of introduction to the relationship between terrorism and the business community, I would like to say a few more words about the overall terrorist threat. These will, I promise, be the only numbers I throw at you tonight.

Terrorism is a growth industry, as the number of incidents increase an average 10 to 12 percent a year. At first glance, the numbers are scary. Risks International, a firm that tracks terrorist incidents around the world, reported a record 2,265 terrorist attacks last year. And 1986, they report, will certainly top this figure. However, the number of these attacks against U.S. targets was only 97 in 1985; in other words, less than five percent of the total.

And where are Americans in most danger? All statistics keepers agree that Latin America, and not the Middle East, has been, and continues to be, the location of most risk, not only in terms of the number of incidents but also their severity. The State Department reports that in 1985 there were 85 terrorist attacks involving U.S. citizens in Latin America, compared with only 16 in the Middle East. Moreover, of the 75 Arab attacks in Europe that same year, only four incidents were against Americans. The majority of Arab attacks were aimed at fellow Arabs. Latin American terrorism has also been more lethal, accounting for about 40 percent more American deaths than the Middle East terrorism.

What does this mean for business? According to Risks
International, there was a worldwide total of 39 attacks involving U.S.
businesses in 1985, primarily bombings. The majority of these attacks
took place in just three countries: Colombia, Peru, and Chile.

These numbers clearly indicate that terrorism is not an omnipresent, overwhelming threat, despite the publicity to the contrary. However, by keeping informed of terrorist locations, methods, and targets, American businessmen should be able to tailor their response to that threat and continue most operations without running unreasonable risks.

STRATEGIES TO COPE WITH TERRORISM

Now let me turn to some of the results of our RAND study of the strategies that corporations employ when they are threatened. As I said earlier, we focused on two countries that underwent periods of extensive terrorist activity during which the host government was unable and/or unwilling to offer adequate protection. These were Argentina from 1969 to 1978, and El Salvador from 1977 to 1981.

Let me give you some indication of what I mean by extreme threat. During 1973, one of the worst years of terrorism against businesses in Argentina, 11 executives of U.S. operations were kidnapped for total ransom demands exceeding \$28 million, 3 American executives were assassinated, and Ford, Pan Am, Braniff, Otis, Coca-Cola, ITT, John Deere, and IBM reported extortion threats. This does not include

bombings and other forms of violence. Moreover, it addresses only attacks on American companies and, therefore, represents only a fraction of the total violence. The strategies that I am presenting, then, are in reaction to a much more severe terrorist environment than businesses normally face.

I would like to add the caveat that just as each terrorist incident is unique, so is each business's experience with terrorism. A number of factors affect that experience, including the type of operation, size, and image of the corporation, and location of its facilities. To give a quick example, when we were talking with local businessmen from El Salvador, a coffee plantation owner complained that he was stuck with few options while his friend, the cattleman, had protected his assets by driving his herds across the border. So what I am about to present are very generalized portrayals of how corporations cope with terrorism.

We found that U.S. businesses have developed four general strategies to deal with terrorist threats. These include the institution of a security program, the promotion of management styles and personnel policies tailored to the risk of dangerous overseas assignment, dealing with the terrorists themselves, and reducing or hedging the assets at risk.

Corporate Security Programs

By far the most frequent and obvious response of U.S. companies was the development of corporate security programs. Because there can be no absolute guarantee against being successfully targeted, the general philosophy of security programs has been to make terrorist operations against their employees and facilities more difficult than operations against other potential targets. Firms increase security as the threat escalates. In all instances, security is a preventive measure and not a solution to the terrorist problem. It may prevent terrorists from choosing a particular target, but it will not necessarily deter them from acting elsewhere. Thus many security personnel we talked to cynically observed that it was their job to make it just a little harder to attack their business so that terrorists would aim their operations at the firm across the street.

Security experts advise that a company's security program has four components: executive protection, security of employees and facilities, intelligence, and crisis management. Briefly, these entail the following.

Many companies have instituted programs to protect their key personnel. One phase usually involves training sessions to enhance the executive's awareness of the threat and to alter behavior patterns that make him an easy target. Thus, the program not only trains executives to spot surveillance and effect evasive tactics, but also encourages them to avoid routinized activities, vary routes into work, and avoid publicity—in other words, adopt a lifestyle less susceptible to attack.

Another aspect of executive protection programs often centers around the traveling executive. Security personnel review itineraries, check out meeting sites, and brief the executive before departure. When the executive is traveling to a threatening environment, security advisors try to find out which hotel has the best security or what is the safest form of transportation.

Finally, the executive protection may also include daily protection of key personnel perceived to be in danger. This may include armored cars, bodyguards, chauffeurs trained in defensive driving, and offices protected from public access.

The second element of the corporate security program deals with the security of the employees and facilities that terrorists have threatened with bombs, strafings, lock-ins, and sabotage. Companies now run security inventories and inspections of their facilities, trying to adjust protective measures to the changing threat.

One company classifies its facility sites according to the environment in which they operate: (1) those in a currently risky environment (El Salvador); (2) those in a country that could soon become risky (Philippines); and (3) those where adverse change would take place only over an extended period of time (Britain). The classification indicates the priority for the allocation of company security resource. First, the company improves the security of sites in immediate danger. Then it improves security in the second and develops contingency plans for the third category of sites.

The third element of the corporate security program is intelligence. While one of the most important functions of the program, it is also the least formalized activity. Corporations usually gather information from an informal network of contacts built on personal relationships. In addition to being used to assess the threat, the information gathered helps the corporation to determine whether the political environment is favorable for additional investments or upgrading present facilities.

Developing local contacts and information is sufficiently important to one company that it assigns an inside and an outside security man to overseas facilities. The main job of the outside man is to cultivate local contacts so that the company will receive good intelligence and local cooperation should an incident occur.

The last component of the corporate security program is a crisismanagement mechanism in the form of a committee of corporate officers
that establishes the corporation's response to a threat. The team
usually includes the chief executive officer or the senior vice
president, the relevant regional division head, a financial officer, a
corporate legal official, personnel representative, public relations or
communication expert, and the corporate security director.

Crisis-management teams, which undergo training by simulating crises, not only react to ongoing problems but can also anticipate problems and develop contingency plans. For example, a corporate subsidiary in Argentina that had already paid off one extortion threat after the murder of an executive, anticipated further trouble. The crisis-management team developed a contingency plan to get its expatriate executives out of the country within 24 hours. The plan included such details as reserving airline seats on a daily basis. When terrorists killed another executive six months later, the contingency plan enabled the company to evacuate its most vulnerable executives from the country the same day.

Proponents of crisis management point out its usefulness in a wide variety of situations from natural disasters to incidents of product tampering to a revolution. In fact, one company we talked to refers to its crisis-management group as the "special events" committee.

Overseas Management Policies

While the corporation can provide a lot of support to local operations through a security program, it is the overseas manager who must really cope with the threat. In both Argentina and El Salvador, management strategies emerged to match the increasing threat but they also progressively separated the manager from his operation. First, the manager takes the established precautions of the executive protection program I have already described. He maintains no established routine. Hours at the office become erratic as he arrives and leaves at irregular times.

As the situation deteriorates, the executive increasingly runs the business by telephone from home. If he is threatened, he takes unannounced trips out of the country or checks into hotels and uses rented cars. He may even, in extreme circumstances, move to a nearby country, conduct business by telephone, and make lightning visits to the local operation by arriving unannounced and departing the same day.

Most frequently, the corporation replaces American executives with country nationals. Because terrorists also target local businessmen, companies still have to provide security protection and other support. However, a local manager is usually not as conspicuous as an American and enhances the image of the company.

Companies have also had to pay more attention to labor relations and personnel policies as terrorists have infiltrated labor unions and offices as well as exploited management-labor disputes. Managers with whom we talked stressed the importance of establishing a dialogue with local employees so that they can understand the company's limitations in terms of jobs, wages, and benefits. In fact, one manager hired a communications specialist to facilitate good relations in his plant. Another company, worried that terrorists were trying to infiltrate their regional headquarters, tended to hire middle-aged secretaries because they did not fit terrorist profiles.

Dealing With the Terrorist

A more risky strategy is to deal with the terrorists themselves. In the Basque province of Spain, firms operate by virtue of a "revolutionary tax" paid to local terrorists. At the other extreme, businessmen contribute financial support to antiterrorist vigilante operations, such as U.S. Ambassador White suggested was the case in El Salvador in 1980.

Reducing the Risk

Finally, many U.S. businesses try to minimize potential losses by hedging their risks. A 1980 study, for example, indicated that 40 to 60 percent of U.S. multinationals now carry kidnap and ransom insurance. Insurance companies are beginning to introduce political risk coverage.

However, companies have found other ways to reduce exposure of their assets. A retail firm in Central America reduced the corporation's assets when the political climate deteriorated by contracting its credit terms, since credit accounts are its chief asset abroad. This same company also tried to reduce its capital investments in Central America. A construction company contracting to work in a high-risk and remote area sold its expensive construction equipment to the local government for the duration of the contract so that the government would assume the risk of damage or destruction by terrorists.

THE COSTS OF TERRORISM

While U.S. businesses have demonstrated that they can not only survive but also prevail in severe terrorist environments, there are a number of costs.

The most obvious are the financial bills associated with upgrading security, hiring guards, purchasing insurance, providing hardship pay, or paying ransoms and "revolutionary taxes." These can be very significant. Round-the-clock protection can cost upwards of \$100,000 per year. Kidnap and ransom insurance, depending on the riskiness of the location, requires premiums ranging from \$100,000 for \$10 million of coverage in the United States to \$500,000 in more dangerous Colombia. Reported property damage and ransoms for U.S. companies last year alone exceeded \$5 million.

As expensive as such security- and threat-related items are, companies may suffer more serious penalties as a result of the very strategies used to cope with terrorism. First, the management styles imposed by erratic hours at the office, unannounced lightning business trips by other corporate officials, or trying to run the operation from home by telephone take their toll on effective management. As one American manager in El Salvador told us, "I became totally preoccupied with security."

There are also disadvantages in moving the executive to a neighboring country. Several executives we talked to in Argentina felt that companies which ran their operations out of Montevideo did not do as well as those who remained in Buenos Aires. Replacing American executives with country nationals also had penalties when the threat necessitated an abrupt change before the replacement received adequate preparation.

Second, corporate embargoes on travel to terrorist environments can also have significant repercussions. During the worst years in Argentina, two American corporations told us they could not maintain routine quality control measures. In El Salvador, one plant could manage only minor repairs to machinery locally, and had to ship the machines back to the United States for major overhauls. Another company reported longer than normal idle times when machines broke down, because of the scarcity of local technicians.

Even more serious, manufacturers became technology-bound because they were unable to send in technicians to set up new lines and train the work force. Companies also were reluctant to put advanced equipment in such a risky environment. A corporation which had updated plants elsewhere found the obsolescence of the Salvadoran facility made it relatively less efficient and more difficult to integrate into the corporation's overall production goals.

The company's response to terrorist threats can have other adverse repercussions beyond the running of the overseas operation. For example, the corporation's attempts to meet terrorists' kidnapping or extortion demands may seriously damage the firm's relations with the government.

In Argentina, corporations had a history of failing to report kidmappings to the local police or security forces, especially when terrorists threatened to retaliate against such action. Companies also felt inhibited from going to the local police when they believed them mept, infiltrated by the terrorists, or likely to engage in a premature confrontation with the terrorists which would endanger the hostage.

More serious than offending the local constabulary, corporate behavior also led to confrontation with the national government. A number of nations have outlawed the publication of manifestos and the payment of ransom and otherwise indicated their opposition to aiding terrorists. They have, on occasion, arrested the corporation's negotiators and threatened other legal reprisals. We ran into a number of examples of this.

A Dutch firm, trying to get an executive released from Salvadoran terrorists, was not allowed by the government to publish ads in Salvadoran newspapers. As an alternative, the firm was forced to pay an estimated \$2 million for advertisements in newspapers throughout the world. In another kidnapping, the Venezuelan government threatened to nationalize Owens-Illinois for acceding to terrorists' demands to publish corporate documents embarrassing to the government.

In probably the most spectacular case, Montoneros kidnapped Juan and Jorge Born, top executives of an Argentine trading conglomerate. Noting that the Montoneros received a \$60 million ransom, the equivalent of one-third of Argentina's defense budget, the Argentine government expressed its dissatisfaction by arresting seven of the conglomerate's executives and launched an investigation to determine whether the company had violated tax or foreign exchange laws in raising the ransom.

Finally, terrorist environments may impose severe penalties to the U.S. business if they contribute to adverse changes in local government policy, such as currency controls, or limitations on foreign ownership. One U.S. firm told us that currency restrictions in El Salvador caused reare problems for their operation than any acts of terrorism. The general instability of that country had caused a run on the local currency as wealthy Salvadorans tried to transfer their assets out of the country. As a result, the local government nationalized the banks,

forcing all payments to be made in local currency, and thus making it much more difficult for U.S.-based businesses to operate to advantage. In a similar vein, FORTUNE magazine recently quoted an oil-drilling company executive, as follows: "By the time the cost of protecting yourself rises to more than 3 percent of the revenues, you are facing a complete breakdown of society, and it is not a question of protection but of running your business. You cannot get raw materials in or finished products out, and the local currency is shot."

Despite the direct or indirect costs terrorism inflicts on a sempany, it would be misleading to overstate the long-term influence of these penalties. We found few corporations which actually shut down their operations as a result--and even when they did it was due to the long-term economic viability of the business. Most corporate officials we talked to consider terrorist threats as episodic events, and they philosophically expect to cope with terrorism just as they continue to operate through times of war and other violence. They understand that many locations which attract investment also foster conditions conducive to terrorist activity, and they accept that risk in order to do business there.

THE HOSTAGE EXPERIENCE

Finally, I would like to talk a little bit about the hostage experience. Businessmen are likely to become hostages under two totally different sets of circumstances: at-large kidnappings or hostage-barricade situations.

The first is the traditional kidnapping in which the whereabouts of the hostage is unknown. It is most likely to be characterized by the following:

- The hostage is specifically targeted after surveillance and research into the company. He is most likely seized from his car going to or coming back from work.
- The kidnappers' demand that the police not be informed results
 in the company or family handling the negotiations.

- The kidnappers usually demand ransom.
- The hostage is likely to be held for a long time. Because the kidn opens want to remain anonymous, negotiations can be drawn out for weeks and even months, as contact with the firm and negotiators is carried on in a circuitous, sporadic fashion. The hostage's incarceration may be lengthened further if the kidnappers insist on laundering the ransom money before releasing the hostage.
- The kidnap victim is most likely the only hostage in circumstances that may resemble solitary confinement. Since kidnappers want to keep their identity a secret, they often wear hoods. Almost every hostage we talked to mentioned the psychological stress of not seeing a human face for long periods.

In contrast, a ho Lage-barricade situation, in which the terrorists have seized hostages publicly, is most likely to be characterized by the following:

- Instead of being specifically targeted, the hostage was probably in the wrong place at the wrong time.
- By definition, security forces have surrounded the kidnappers and hostages, and local government officials are running the negotiations.
- Because the situation is basically one of confrontation in which the security forces control the outside environment-i.e., food, electricity, telephone--the incident is most likely to be counted in hours or days, punctuated by a series of shortterm deadlines.
- The most likely demands are political in nature--usually the release of prisoners.
- The hostage is most likely one of many.

Although there are major differences in these two kinds of experiences, terrorism experts agree that some general, interrelated guidelines apply to both situations:

- Keep your head--terrorists are likely to panic fairly easily and you do not want to precipitate action on their part.
- Do not put up a fight; cooperate. Most deaths occur during the seizure of the hostages.
- Do not try to escape--unless you are really sure of success or all hell breaks loose.
- If possible, keep yourself fit by eating well and exercising.
 This aids in keeping alert and fending off depression during captivity.

The descriptions many hostages give of their experience often resemble that joke definition of boating as hours of boredom punctuated by moments of sheer panic. Victims of at-large kidnappings are often held for weeks or even months in limbo--having no contact with the outside world and often no one to talk with. One ex-hostage, held for five months in an underground cell, told us he used to do everything very, very slowly to help fill the time. Most devise schedules for themselves to get through the day. Even victims of hostage-barricade situations often are not allowed to talk among themselves and/or have been bound up. Moreover, they, too, often have little knowledge of events going on around them. Under such conditions, the waiting period becomes excruciating.

Some hostages experience what is popularly known as the Stockholm syndrome. Napolean Duarte's daughter is one of the most recent victims of this syndrome, in which the hostage demonstrates positive feelings toward his captors and negative ones toward the security forces. Psychologists theorize this happens for a number of reasons. The hostage perceives that his survival depends on the safety of his captors. The close quarters of the hostages and terrorists promote a group encounter experience. Because the kidnappers have complete control over the hostage's life, deciding in fact if he will live or die, the hostage begins to identify with his captors.

However, there is a reverse Stockholm syndrome, i.e., captors senetimes become attached to their hostages. One of the best strategies to enhance survival is to become a human being in the eyes of your captors, not just a bargaining chip. The ability to employ this strategy can be limited if the hostage does not speak the same language or is not allowed to speak. However, if hostages can communicate aspects of their lives--families, dreams, disappointments--they make it more difficult for the terrorists to harm them.

While the hostage experience is very traumatic, many find the aftermath also holds many terrors. Symptoms of readjustment problems include insomnia, nightmares, tremors, impotence, loss of appetite, restlessness, difficulties in concentration, and alienation.

One of the most difficult aspects of the aftermath is coming to terms with how you acted during captivity. Many victims are hard on themselves—they should not have been captured, they should not have cooperated so much, or they were not as brave as they would have liked. This can engender a self—imposed sense of guilt. Ironically, others may reinforce this feeling by treating ex-hostages like rape victims—i.e., they want to deny that it could happen to them so they make it the victim's fault that he was captured.

Psychiatrists feel that victims of terrorism may also have more trouble than other victims because terrorists usually get away scotfree. There is no sense of a just end. The fact that terrorists usually get away may also contribute to the exaggerated fears which continue long after the event. One hostage, after being kidnapped in the Middle East, returned to California, where he bought a house at the end of a dead-end street with woods beyond. For almost a year after his kidnapping, if a car drove within three houses, he would go out the back door into the woods. He just was not going to get captured again.

For some ex-hostages, the experience triggers changes in lifestyles and careers. In one well-publicized example, the chairman of a French manufacturing firm was held hostage for 63 days during which he was threatened with death and lost the tip of one finger (sent to his family as proof of his identity). At the time of his release, the hostage said that "the thing I regretted during my captivity was not having taken

sufficient advantage of life, not having seen enough places, known enough girls." He subsequently embarked on a playboy tour of the United States, and after seven months shed some of his flamboyance and returned to France to run his company.

As these examples illustrate, reactions vary widely. But in all events, companies must be prepared to offer medical and psychological help as well as patience and understanding after employees have been kidnapped.

In conclusion, I would like to say that after all my research and interviews, I am optimistic that U.S. businessmen can pursue their interests abroad even when terrorism threatens. While terrorists find Americans and their corporations attractive targets, the threat is by no means worldwide, but rather in specific locations, by specific groups. By keeping track of terrorist methods and structuring corporate measures to counter the threat, overseas operations become less attractive targets and terrorists are likely to look for easier prey.

In a severely threatening environment, when the host government cannot guarantee the country's internal security, companies have developed a number of strategies to continue operating, although not without some cost and penalties. However, most terrorism is episodic, and U.S. corporations have maintained their overseas operations long after the terrorist groups threatening them have gone.

END DATE FILMED DT/C 1-88